THE ARITHMETIC OF PRYM VARIETIES IN GENUS 3

NILS BRUIN

Abstract. Given a curve of genus 3 with an unramified double cover, we give an explicit description of the associated Prym variety. We also describe how an unramified double cover of a non-hyperelliptic genus 3 curve can be mapped into the Jacobian of a curve of genus 2 over its field of definition and how this can be used to do Chabauty- and Brauer-Manin type calculations for curves of genus 5 with an unramified involution. As an application, we determine the rational points on a smooth plane quartic with no particular geometric properties and give examples of curves of genus 3 and 5 violating the Hasse-principle. We also show how these constructions can be used to design smooth plane quartics with specific arithmetic properties. As an example, we give a smooth plane quartic with all 28 bitangents defined over $\mathbb{Q}(t)$, By specialization, this also gives examples over $\mathbb{Q}$.

1. Introduction

In this article, we investigate the arithmetic of unramified double covers of non-hyperelliptic curves of genus 3. This research is inspired by the recent success in applying the theory of unramified double covers to hyperellipitic curves to the problem of determining the set of rational points on such curves ([25], [4], [5], [7]). Combined with explicit Chabauty-methods, this has yielded very practical methods for obtaining often sharp bounds on the number of rational points on a hyperelliptic curve. In the hyperelliptic case, the construction of unramified covers is particularly easy to make explicit using Kummer theory. There has been some limited work investigating how these ideas may be generalised to unramified covers of higher degree of hyperelliptic curves ([3]).

In this article, we generalise in a different direction. We derive the general form of a curve C of genus 3 over a field K of characteristic 0 that allows an unramified double cover $\pi : D \to C$ defined over K. A non-hyperelliptic curve of genus 3 with an unramified double cover allows a smooth plane projective model of the form

$$C : Q_1(u,v,w)Q_3(u,v,w) = Q_2(u,v,w)^2$$

where $Q_1, Q_2, Q_3 \in K[u,v,w]$ are quadratic forms. The unramified double cover has a canonical model in $\mathbb{P}^5$ of the form

$$D : \begin{cases} Q_1(u,v,w) &=& r^2 \\ Q_2(u,v,w) &=& rs \\ Q_3(u,v,w) &=& s^2\,. \end{cases}$$

Date: May 30, 2006.

1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 14H40.

Key words and phrases. Prym varieties, Chabauty methods, rational points on curves, covering techniques, Brauer-Manin, smooth plane quartics.

The research in this paper is partially supported by NSERC.

We also describe how the associated Prym variety (the connected component containing 0 of the kernel of $\pi_* : \mathrm{Jac}(D) \to \mathrm{Jac}(C)$) can be described explicitly as $\mathrm{Jac}(F)$ of some genus 2 curve F over K:

$$F : y^2 = -\det(Q_1 + 2xQ_2 + x^2Q_3)$$

where we regard Q_i as the symmetric 3×3 matrices corresponding to the quadratic forms they represent. Combined with earlier work, this gives a complete description of how principally polarised Abelian surfaces arise as Prym varieties in genus 3 over non-algebraically closed base fields of characteristic 0 (see Theorem 5.1).

The description of $\mathrm{Prym}(D/C)$ as $\mathrm{Jac}(F)$ over $\mathbb{C}$ can already be found in [1, Exercise VI.F]. Alternatively, if C has a rational point, then the *trigonal construction* gives a Galois-theoretic way of describing the Prym variety as the Jacobian of some curve (see [12] and [20]). Here, we refine the description to arbitrary characteristic 0 base fields. The results should generalise to arbitrary odd characteristic.

We show how D can be mapped into $\mathrm{Prym}(D/C)$ over K, without additional assumptions on D (see Proposition 6.2). We can thus use Chabauty-like methods on genus 5 curves in Abelian surfaces to get an in practice often sharp bound on the number of rational points on D. This can in turn be used to get a corresponding bound on the number of rational points on C. As an example, we prove

Proposition 1.1. *For the curve*

$$C : (4u^2 - 4vw + 4w^2)(2u^2 + 4uv + 4v^2) = (2u^2 + 2uw - 4vw + 2w^2)^2$$

we have $C(\mathbb{Q}) = \{(0 : 1 : 0)\}$.

The proof avoids computing the Mordell-Weil group of $\mathrm{Jac}(C)$. Instead, it uses the computationally more accessible Mordell-Weil group of an Abelian surface.

Furthermore, the method does not put restrictions on the geometry of C: Over some field extension L, the group scheme $\mathrm{Jac}(C)[2]$ has a non-trivial rational point and therefore an unramified cover D of the desired type and a map $D \to \mathrm{Prym}(D/C_L)$. In complete analogy to the treatment of genus 2 in [5], by taking the Weil-restriction of scalars, we obtain $\Re_{L/K}(D) \to \Re_{L/K}(\mathrm{Prym}(D/C_L))$. Inside of $\Re_{L/K}(D)$, we can find a curve $\tilde{D}$ corresponding to $\Re_{C_L/C_K}(D/C_L)$. We can then apply Chabauty-like methods to $\tilde{D} \to \Re_{L/K}(\mathrm{Prym}(D/C_L))$ to determine $\tilde{D}(K)$ and $C(K)$. The group $\Re_{L/K}(\mathrm{Prym}(D/C_L))(K) \simeq \mathrm{Prym}(D/C_L)(L)$ would be the hardest ingredient to obtain and it should be noted that the computations involved would probably be prohibitive, except for very low degree L.

Since the mapping of D into $\mathrm{Prym}(D/C)$ does not require a rational point on D, we can apply this construction to prove that $D(\mathbb{Q})$ is empty, even if D does have points everywhere locally. It is reassuring that, at least conjecturally, our computations correspond to determining part of the Brauer-Manin obstruction of D:

Suppose that D is a curve of genus larger than 1, defined over a number field K, with points everywhere locally. Assuming $Ш(\mathrm{Jac}(D)/K)$ is finite, a failure for D to have a K-rational degree 1 divisor class would be due to the Brauer-Manin obstruction (see [23, Corollary 6.2.5]). Otherwise, using an Abel-Jacobi embedding, D can be considered a subvariety of $\mathrm{Jac}(D)$. Scharaschkin [22] proves that if $D(\mathbb{A}_K)$ misses the topological closure of $\mathrm{Jac}(D)(K)$ in $\mathrm{Jac}(D)(\mathbb{A}_K)$, then this is due to the Brauer-Manin obstruction on D if $Ш(\mathrm{Jac}(D)/K)$ is finite.

In our computations, we show that the image of $D(\mathbb{A}_\mathbb{Q})$ in $\mathrm{Prym}(D/C)(\mathbb{A}_\mathbb{Q})$ misses the closure of $\mathrm{Prym}(D/C)(\mathbb{Q})$ by combining the local information at a finite number of primes.

As an example, we prove

Proposition 1.2. *The genus* 5 *curve*

$$D : \begin{cases} (v^2+vw-w^2) &=& r^2 \\ (u^2-v^2-w^2) &=& rs \\ (uv+w^2) &=& s^2 \end{cases}$$

and the genus 3 *curve*

$$C : (v^2+vw-w^2)(uv+w^2) = (u^2-v^2-w^2)^2$$

both have points everywhere locally, but they have no rational points.

For this example, we find $\mathrm{Prym}(D/C)(\mathbb{Q}) \simeq \mathbb{Z}\times\mathbb{Z}$. This illustrates that the method used is not a special case of a Chabauty-type argument.

Additionally, we investigate the arithmetic implications of the geometric description of the fibres of the Prym map between moduli spaces, corresponding to the functor $\{\pi : D \to C\} \mapsto \{\mathrm{Prym}(D/C)\}$, given in [24]. For a general Abelian surface A, the Kummer surface $\mathcal{K} = A/\langle\pm 1\rangle$ has a singular quartic model in $\mathbb{P}^3$, with a singular locus consisting of 16 points, corresponding to $A[2]$. Translation by $A[2]$ induces automorphisms on $\mathcal{K}$, given by linear transformations on $\mathbb{P}^3$. We write $\widehat{\mathbb{P}}^3$ for the space of planes in $\mathbb{P}^3$. Verra [24] shows that over $\mathbb{C}$, the fibre of the Prym map over a principally polarised surface A, is birational to $\widehat{\mathbb{P}}^3/A[2]$. In fact, he gives a very precise description of the fibre as a blow-up of this space, where the exceptional components contain the moduli points corresponding to hyperelliptic or otherwise degenerate curves C.

In particular, a non-hyperelliptic genus 3 curve C over $\mathbb{C}$ which has a double cover D such that $\mathrm{Prym}(D/C) = A$ can be obtained as a plane section of $\mathcal{K}$, with D the pull-back of C to A. Any two such plane sections of $\mathcal{K}$ in the same $A[2]$-orbit give isomorphic covers D/C.

In this article we explain how, given a genus 2 curve F over a number field K and a genus 3 plane section C of $\mathcal{K} = \mathrm{Jac}(F)/\langle\pm 1\rangle$, we can obtain a model for C of the type $Q_1Q_3 = (Q_2)^2$. Since a sufficiently general plane section of $\mathcal{K}$ is non-singular and thus of genus 3, it shows that any Jacobian of a genus 2 curve over K can be realised as a Prym variety of a non-hyperelliptic genus 3 curve *over* K, or stated more amusingly in an elementary fashion:

Proposition 1.3. *Let $f \in \mathbb{Q}[x]$ be a square-free polynomial of degree* 5 *or* 6*. Then there exist symmetric matrices $M_1, M_2, M_3 \in \mathbb{Q}^{3\times 3}$ such that*

$$f = \det(M_1 + xM_2 + x^2M_3).$$

We use this construction to obtain a systematic way of constructing curves of genus 3 with all 28 bitangents defined over a non-algebraically closed field, for instance $\mathbb{Q}(t)$ (see Section 7). By specialisation of t, this gives infinitely many examples over $\mathbb{Q}$. This strenghtens a result in [13], where an example is given with all bitangents defined over $\mathbb{R}$. See [21] or [9] for an approach via interpolation.

Finally, it should be noted that not all covers $\pi : D \to C$ defined over K with $\mathrm{Prym}(D/C) = A$ and C non-hyperelliptic have C occurring as a plane section of the associated Kummer surface $\mathcal{K}$ defined over K, since not all rational points of

$\widehat{\mathbb{P}}^3/A[2]$ are covered by rational points of $\widehat{\mathbb{P}}^3$. In particular, the 16 tropes of $\mathcal{K}$ give rise to a Galois-stable set of 16 bitangents to C. Not all smooth plane quartics have such a configuration of bitangents.

2. Preliminaries

First we fix some notation. Let K be a field and let C be a complete, absolutely irreducible algebraic curve over K. We write κ_C for a canonical divisor on C. For a divisor $\mathfrak{D} \in \mathrm{Div}(C)$, we write $[\mathfrak{D}]$ for its class in $\mathrm{Pic}(C)$ and $|\mathfrak{D}|$ for the complete linear system corresponding to $\mathfrak{D}$ and $l(\mathfrak{D}) = \dim|\mathfrak{D}|$. We say that a divisor $\mathfrak{D}$ on C is a g_d^r if $\deg(\mathfrak{D}) = d$ and $l(\mathfrak{D}) > r$. We write $W_d^r \subset \mathrm{Pic}^d(C)$ for the classes of g_d^rs. By abuse of notation, we will also write W_d^r for the corresponding subscheme of the scheme representing the functor $\mathrm{Pic}^d(C)$.

2.1. Unramified double covers and Prym varieties.

Let $\pi : D \to C$ be an unramified finite morphism of degree 2 between curves over a field K and let $\iota : D \to D$ be the involution of D over C. It follows by Riemann-Hurwitz that $g(C) > 0$ and that

$$g(D) = 2g(C) - 1.$$

The kernel of $\pi_* : \mathrm{Jac}(D) \to \mathrm{Jac}(C)$ has two connected components. The component that contains 0 coincides with the image of $(\mathrm{id}_* - \iota_*) : \mathrm{Jac}(D) \to \mathrm{Jac}(D)$.

Definition 2.1. Let $\pi : D \to C$ be an unramified finite morphism of degree 2 between curves over a field K. We write $\mathrm{Prym}(\pi) = \mathrm{Prym}(D/C)$ for the connected component of the identity-element of $\ker(\pi_* : \mathrm{Jac}(D) \to \mathrm{Jac}(C))$. We call this the *Prym variety* of D/C.

Thus, $\mathrm{Prym}(D/C)$ is an Abelian subvariety of $\mathrm{Jac}(D)$. The principal polarisation on $\mathrm{Jac}(D)$ restricts to a principal polarisation on $\mathrm{Prym}(D/C)$. Historically, Prym varieties were considered interesting primarily because they give examples of principally polarised Abelian varieties that are not Jacobian varieties. However, if $\dim(\mathrm{Prym}(D/C)) \leq 2$, then $\mathrm{Prym}(D/C)$ generally is a Jacobian variety[1]. See [1, VI-C] or [19] for details.

2.2. Prym varieties in the hyperelliptic case.

Contrary to the general situation, the Prym variety associated to an unramified double cover of a hyperelliptic curve is closely related to a Jacobian variety. In fact, the Prym variety is isomorphic to the product of Jacobian varieties of subcovers, which themselves are again hyperelliptic.

Let us first assume that C is a double cover of a $\mathbb{P}^1$. Then C has an affine model of the form

$$C : y^2 = f(x)$$

where $f \in K[x]$ is a square-free polynomial of degree $2g(C) + 2$. Kummer theory tells us exactly what the unramified degree 2 extensions of $K(C)$ are. For any factorisation $f = f_1 f_2$, with $f_1, f_2 \in K[x]$ and of even degree, we have a curve D given by the affine model

$$\begin{cases} y_1^2 &= f_1(x) \\ y_2^2 &= f_2(x) \end{cases}$$

[1] It can also be the product of two elliptic curves, in which case it is a generalised Jacobian.

and an unramified morphism of degree 2

$$\begin{array}{cccccc} \pi & : & D & \to & C & \\ & & (x, y_1, y_2) & \mapsto & (x, y_1 y_2) & = (x, y). \end{array}$$

Then there are the two obvious curves

$$\begin{array}{rcl} F_1 : \ y_1^2 & = & f_1(x) \\ F_2 : \ y_2^2 & = & f_2(x). \end{array}$$

with the obvious projections $\pi_1 : D \to F_1$ and $\pi_2 : D \to F_2$. This yields the familiar diagram associated to biquadratic extensions.

$$\begin{tikzcd} & D \arrow[dl, "\pi_1"'] \arrow[d, "\pi"] \arrow[dr, "\pi_2"] & \\ F_1 \arrow[dr, "x"'] & C \arrow[d, "x"] & F_2 \arrow[dl, "x"] \\ & \mathbb{P}^1 & \end{tikzcd}$$

Proposition 2.2. *Let $C, D, F_1, F_2, \pi, \pi_1, \pi_2$ be defined as above. Then*

$$\pi_1^* \times \pi_2^* : \mathrm{Jac}(F_1) \times \mathrm{Jac}(F_2) \to \mathrm{Prym}(D/C)$$

is an isomorphism of Abelian varieties.

Proof. First, we prove that π_1^* indeed maps $\mathrm{Jac}(F_1)$ into $\mathrm{Prym}(D/C)$. To that end, take the generic point $(x_1, y_1) \in F_1$. We have $\pi_1^*(x_1, y_1) = (x_1, y_1, \sqrt{f_2(x_1)}) + (x_1, y_1, -\sqrt{f_2(x_1)})$. Under π, this maps to the divisor cut out by $x = x_1$. This shows that $\pi_* \pi_1^* : \mathrm{Jac}(F_1) \to \mathrm{Jac}(C)$ is constant and hence $(\pi_* \pi_1^*)|_{\mathrm{Jac}(F_1)}$ is the zero map. By symmetry it follows that $\mathrm{Jac}(F_1) \times \mathrm{Jac}(F_2)$ lands in the kernel of π_* under $\pi_1^* + \pi_2^*$ and, since it is connected and covers $0 \in \mathrm{Jac}(D)$, lands in $\mathrm{Prym}(D/C)$.

The fact that $(\pi_i)_* \circ \pi_i^* = 2|_{\mathrm{Jac}(F_i)}$ for $i = 1, 2$ already assures that $\mathrm{Jac}(F_1) \times \mathrm{Jac}(F_2)$ is isogenous to $\mathrm{Prym}(D/C)$. A quick way to see that they are actually isomorphic is by noting that F_1 and F_2 can be arbitrary hyperelliptic curves and that, by construction, the isogeny would have to depend functorially on F_1 and F_2. In general, $\mathrm{Jac}(F_1) \times \mathrm{Jac}(F_2)$ has no non-trivial polarisation-preserving isogenies and hence there are no other candidates for $\mathrm{Prym}(D/C)$. $\square$

Remark 2.3. There are more complicated situations than the split situation described in 2.2. For instance, if L is a quadratic extension of K with conjugation $\sigma : L \to L$ over K and $f_2 = {}^\sigma f_1$, then $F_2 = {}^\sigma F_1$. There is still an unramified double cover D/C over K associated with this splitting. The corresponding Prym variety is the Weil restriction $\Re_{L/K} \mathrm{Jac}(F_1)$.

Remark 2.4. In general, a hyperelliptic curve C over K is a double cover of a curve L of genus 0. We can express $K(L)$ as some quadratic extension of $K(\mathbb{P}^1)$. Relative Kummer theory allows us to describe $\mathrm{Prym}(D/C)$ in terms of Jacobians of subcovers of D/L in exactly the same way as above.

2.3. **Linear subspaces on quadrics.** It is well known that on a non-singular quadric in $\mathbb{P}^3$, there are two rulings of lines with the property that a line from one ruling intersects a unique line from the opposite ruling and that two lines from the same ruling do not intersect. We will need a simple lemma that classifies whether the two rulings are split or quadratic conjugates.

Lemma 2.5. *Let K be a field of characteristic different from 2 and let $M \in K^{4\times 4}$ be a symmetric matrix describing a non-singular quadric $Q \subset \mathbb{P}^3$. The two rulings of lines on Q are individually defined over K exactly if $\det(M)$ is a square in K. Otherwise, they are quadratic conjugate.*

Proof. First assume we have a point $\mathbf{x}_0 \in Q(K)$. Let $V = \{\mathbf{x} : {}^t\mathbf{x}_0 M\mathbf{x} = 0\}$ be the plane tangent to Q at $\mathbf{x}$. The intersection $V \cap Q$ consists exactly of two lines through $\mathbf{x}_0$, one from each of the rulings. With a change of basis, we can assume that $\mathbf{x}_0 = (1 : 0 : 0 : 0)$ and that the points $\mathbf{x}_1 = (0 : 1 : 0 : 0)$ and $\mathbf{x}_2 = (0 : 0 : 1 : 0)$ lie on V as well. It follows that

$$M = \begin{pmatrix} 0 & 0 & 0 & d \\ 0 & a & b & * \\ 0 & b & c & * \\ d & * & * & * \end{pmatrix}; \quad \det(M) = d^2(b^2 - ac)$$

We see that Q intersected with the line through $\mathbf{x}_1, \mathbf{x}_2$ is described by the equation $ax_1^2 + 2bx_1x_2 + cx_2^2 = 0$, which is split exactly if $b^2 - ac$ is a square. The lemma follows.

If $Q(K)$ is empty, then we base change to $K(Q)$, where we have the generic point $(x_0 : x_1 : x_2 : x_3) \in Q(K(Q))$. Since K is algebraically closed in $K(Q)$, the pair of rulings (defined over K) is split over $K(Q)$ if and only if they are split over K. Furthermore, $\det(M)$ is a square in K if and only if it is in $K(Q)$. □

3. Non-hyperelliptic curves of genus 5 with an unramified involution

Let K be a field of characteristic 0 and let D be a non-hyperelliptic curve of genus 5 with an unramified involution ι. Let $\pi : D \to C = D/\langle\iota\rangle$ be the quotient map by the action of ι. The Riemann-Hurwitz formula yields that C is of genus 3. Let κ_C be a canonical divisor on C and let $\langle u, v, w\rangle = |\kappa_C|$ be coordinates on the associated canonical model of C. Note that we do not insist that C is non-hyperelliptic. By abuse of notation, we also write u, v, w for the pull-backs along π of the corresponding functions on C. We write $\kappa_D = \pi^*\kappa_C$. There are functions r, s on D with $r + r \circ \iota = s + s \circ \iota = 0$ such that $\langle u, v, w, r, s\rangle = |\kappa_D|$.

We identify D with the canonical model associated to κ_D, being the image of $(u : v : w : r : s) : D \to \mathbb{P}^4$. In this notation,

$$\iota : (u : v : w : r : s) \mapsto (u : v : w : -r : -s).$$

We let Λ be the linear system of quadrics containing $D \subset \mathbb{P}^4$. A simple comparison of the dimensions of $l(\kappa_D) = 5$ and $l(2\kappa_D) = 12$ yields that $\Lambda \simeq \mathbb{P}^2$. Let $Q_1, Q_2, Q_3 \in \Lambda(K)$ be quadrics generating Λ and let $(\lambda_1 : \lambda_2 : \lambda_3)$ be the corresponding coordinates on Λ.

Note that $|\kappa_D|$ has a decomposition in the $+1$-eigenspace $\langle u, v, w\rangle$ and the -1-eigenspace $\langle r, s\rangle$ of ι. The involution ι acts identically on the corresponding linear subspaces $\{r = s = 0\}, \{u = v = w = 0\} \subset \mathbb{P}^4$.

Lemma 3.1. *With the notation above, D is not a trigonal curve.*

Proof. Since a trigonal curve remains trigonal upon base extension, it suffices to prove the lemma for algebraically closed K.

We argue following [1, p. 207]. Suppose that $\mathfrak{D} \in \mathrm{Div}(D)$ is a g^1_3. Then $\kappa_D - \mathfrak{D}$ is a g^2_5, so D has a plane quintic model. This model must have a unique singularity P_0 and the divisors in $|\mathfrak{D}|$ are cut out by lines through P_0.

As is argued in [1, p. 207] (using the Brill-Noether Residue Theorem, see for instance [17, Ch. 8]), a curve of genus 5 can have at most 1 divisor class of type g^1_3. Assume that D is trigonal and let $\mathcal{D}$ be the divisor class of type g^1_3. Then $\iota_* : \mathrm{Div}(D) \to \mathrm{Div}(D)$ induces an involution on $|\mathcal{D}| \simeq \mathbb{P}^1$. Let $\varphi = \varphi_{\mathcal{D}} : D \to \mathbb{P}^1$ be the trigonal map on D. Then $D \to |\mathcal{D}|$ defined by $P \mapsto \varphi^*(\varphi(P))$ shows that $|\mathcal{D}|$ is naturally the $\mathbb{P}^1$ of which D is the degree 3 cover.

Since $|\mathcal{D}|$ contains all effective g^1_3s on D, the restriction of ι^* to $|\mathcal{D}|$ yields an involution on $|\mathcal{D}|$. Since involutions on $\mathbb{P}^1$ have two fixed points, there are two effective g^1_3s on D on which are fixed under ι_*. It follows that ι permutes the support of one such divisor, which consists of 3 not necessarily distinct points. Since $\iota^2 = 1$, it follows that at least one point is fixed under ι and hence that π has ramification. □

Lemma 3.2. *With the notation above, $D = Q_1 \cap Q_2 \cap Q_3$. Furthermore, the Q_i can be chosen to be non-singular and D misses the singular locus of any quadric containing D.*

Proof. First note that if the statement of the lemma is false, then it is also false over the algebraic closure of K. Therefore, it suffices to prove the lemma for algebraically closed K. By Petri's Theorem [1, p. 131], a canonical model of a non-hyperelliptic, non-trigonal curve of genus 5 is the intersection of quadrics.

Next we show that a quadric $Q \in \Lambda$ cannot be singular at D. Suppose that $P_0 \in D$ is a singular point of some quadric $Q \in \Lambda$. Note that, if $\mathrm{rk} Q < 3$, then there is a $\mathbb{P}^3 \subset Q$. The space Λ restricted to that $\mathbb{P}^3$ would be at most a pencil of quadrics and hence contain an intersection of 2 quadrics. This would imply that D has a component of genus at most 1, which contradicts that D is a curve of genus 5.

Hence, Q is of rank 3 or 4, which implies that Q contains a $\mathbb{P}^1$ of planes through the singular point $P_0 \in D$. On each such plane V, the restriction of Λ is a pencil of conics and hence has a base locus of degree 4. Since $P_0 \in V \cap D$ is contained in that base locus, this realises D as a degree 3 cover of that $\mathbb{P}^1$. This contradicts that D is non-trigonal.

By Bertini's Theorem [18, III, 10.9.2] it follows that a general member of Λ is non-singular and hence we can choose the Q_i to be non-singular. □

Lemma 3.3. *With the notation above, we have that ι acts trivially on Λ. Equivalently, for $Q \in \Lambda$, we can find quadratic forms $Q^+ \in K[u, v, w]$ and $Q^- \in K[r, s]$ such that Q is given by the equation*

$$Q^+(u, v, w) + Q^-(r, s) = 0.$$

Proof. First note that ι preserves D and hence preserves Λ. Suppose there is $Q \in \Lambda(\overline{K})$ such that $Q \neq \iota(Q)$. Then $Q - \iota(Q) \in \Lambda(\overline{K})$ is not 0. On the other hand, since ι acts trivially on $\{r = s = 0\}$, we have that $Q - \iota(Q)$ restricted to $\{r = s = 0\}$ is zero. Hence, Λ restricted to $\{r = s = 0\}$ is a pencil of plane conics

and has a base locus of degree 4. It follows that ι is ramified, which contradicts the assumptions.

For an equation of any quadric in $\Lambda(\overline{K})$, this means that the monomials $ur, vr, \ldots, ws$ cannot occur. $\square$

4. Special divisor classes of degree 4

As in the previous section, let D be a non-hyperelliptic curve of genus 5 over a field K of characteristic 0 with an unramified involution $\iota : D \to D$. We adopt the other notation from the previous section as well. We consider the scheme of special divisors

$$W_4^1(D) = \{\mathcal{D} \in \mathrm{Pic}^4(D) : l(\mathcal{D}) \geq 2\}.$$

From the Riemann-Roch formula it follows that the residuation map $\mathcal{D} \mapsto [\kappa_D] - \mathcal{D}$ defines an involution on W_4^1.

We denote the locus of singular quadrics in Λ by

$$\Gamma = \{Q \in \Lambda : \det(Q) = 0\}.$$

By Lemma 3.3 we have a decomposition $\Gamma = \Gamma^+ \cup \Gamma^-$, with equations

$$\begin{array}{rlcl} \Gamma^+ : & \det(\lambda_1 Q_1^+ + \lambda_2 Q_2^+ + \lambda_3 Q_3^+) & = & 0, \\ \Gamma^- : & \det(\lambda_1 Q_1^- + \lambda_2 Q_2^- + \lambda_3 Q_3^-) & = & 0. \end{array}$$

By Lemma 3.2, Γ is 1-dimensional. In fact, it is straightforward to check that

$$\Gamma' = \{Q \in \Lambda : \mathrm{rk} Q = 3\}$$

is 0-dimensional and is the singular locus of Γ.

Lemma 4.1. *Let $\mathfrak{D}, \mathfrak{D}' \in \mathrm{Div}(D)$ be effective divisors of degree 4 with $l(\mathfrak{D}) = 2$. Then the following hold.*

(i) *There is a unique 2-plane $V_{\mathfrak{D}}$ such that $\mathfrak{D} = D \cdot V_{\mathfrak{D}}$.*
(ii) *There is a unique quadric $Q_{\mathfrak{D}} \in \Lambda$ which vanishes on $V_{\mathfrak{D}}$. In fact, $Q_{\mathfrak{D}} \in \Gamma$.*
(iii) *If $V_{\mathfrak{D}}$ and $V_{\mathfrak{D}'}$ meet in a line, then $[\mathfrak{D} + \mathfrak{D}'] = [\kappa_D]$.*
(iv) *If $Q_{\mathfrak{D}} = Q_{\mathfrak{D}'}$ then $[\mathfrak{D}' + \mathfrak{D}] = [\kappa_D]$ or $[\mathfrak{D} - \mathfrak{D}'] = 0$.*
(v) *If $Q_{\mathfrak{D}} \neq Q_{\mathfrak{D}'}$ then $[\mathfrak{D}' + \mathfrak{D}] \neq [\kappa_D]$ and $[\mathfrak{D} - \mathfrak{D}'] \neq 0$.*

Proof. (i): The geometric formulation of the Riemann-Roch Theorem [1, p. 12] states that, for a divisor $P_1 + \cdots + P_r$ with $r \leq g$, we have

$$l(P_1 + \cdots + P_r) = r + 1 - \mathrm{rk}\langle P_1, \ldots, P_r\rangle,$$

so one can take $V_{\mathfrak{D}}$ to be the plane spanned by the support of $\mathfrak{D}$ over $\overline{K}$.

(ii): Since the restriction of Λ to $V_{\mathfrak{D}}$ has a base locus of degree 4, it is a pencil of conics. Hence there is a unique quadric $Q_{\mathfrak{D}} \in \Lambda$ that vanishes on $V_{\mathfrak{D}}$. Since a quadric in $\mathbb{P}^4$ containing a 2-plane is necessarily singular, it follows that $Q_{\mathfrak{D}} \in \Gamma$.

(iii): Two 2-planes meeting in a line lie in a 3-plane, say W. Since $\mathfrak{D} + \mathfrak{D}'$ is effective of degree 8 it equals the hyperplane section $D \cdot W$. Hyperplane sections of canonical models are canonical divisors.

(iv): First suppose that $Q_{\mathfrak{D}}$ is of rank 4. Then $Q_{\mathfrak{D}}$ is a cone over a nonsingular quadric in $\mathbb{P}^3$. The two line rulings on that quadric give rise to two plane "rulings" on $Q_{\mathfrak{D}}$. Planes in opposite rulings meet in a line and planes in the same ruling meet only in the singular point of $Q_{\mathfrak{D}}$. Hence, if $V_{\mathfrak{D}}$ and $V_{\mathfrak{D}'}$ belong to opposite rulings, then by (iii) we have $[\mathfrak{D} + \mathfrak{D}'] = [\kappa_D]$. If $V_{\mathfrak{D}}$ and $V_{\mathfrak{D}'}$ belong to the same

ruling then both $\mathfrak{D}$ and $\mathfrak{D}'$ are residual to an arbitrary divisor from the opposite ruling and hence linearly equivalent.

If $Q_{\mathfrak{D}}$ is of rank 3 then $Q_{\mathfrak{D}}$ is a cone over a singular quadric in $\mathbb{P}^3$, so there is one ruling of planes on $Q_{\mathfrak{D}}$ and any two of these meet in a line. It follows by (iii) that $[\mathfrak{D}+\mathfrak{D}'] = [\kappa_D]$. Since this holds for any $\mathfrak{D}'$ with $Q_{\mathfrak{D}'} = Q_{\mathfrak{D}}$, it follows that that $[\mathfrak{D}-\mathfrak{D}'] = 0$.

(v): Given $V_{\mathfrak{D}}$, there is a map

$$\mathbb{P}^1 \to \{\text{planes in } Q_{\mathfrak{D}}\}$$

parametrising the ruling on $Q_{\mathfrak{D}}$ containing $V_{\mathfrak{D}}$. Each of the planes V in the image of this map cuts out an effective divisor $\mathfrak{D}'$ equivalent to $\mathfrak{D}$. By construction, $Q_{\mathfrak{D}'} = Q_{\mathfrak{D}}$. This gives an explicit realisation of $\mathbb{P}^1 \simeq |\mathfrak{D}|$, so this accounts for all divisors linearly equivalent to $\mathfrak{D}$.

□

Corollary 4.2. *The map*

$$\begin{array}{ccc} W^1_4(D) & \to & \Gamma \\ [\mathfrak{D}] & \mapsto & Q_{\mathfrak{D}} \end{array}$$

is well-defined and realises $W^1_4(D)$ as a double cover of Γ, ramified over Γ'. The involution of $W^1_4(D)$ over Γ corresponds to the residuation map $\mathcal{D} \mapsto [\kappa_D] - \mathcal{D}$.

5. The Prym variety in genus 3.

We write F for the union of components of $W^1_4(D)$ above Γ^-. If $\mathcal{D} \in F$ then $Q_{\mathcal{D}}$ has a singular point on $\{u = v = w = 0\}$. Since the plane $V_{\mathcal{D}}$ passes through this singularity, we see that $\pi(V_{\mathcal{D}})$ is a line and hence that $\pi_*(\mathcal{D}) = [\kappa_C]$. It follows that the map

$$\begin{array}{ccc} F \times F & \to & \mathrm{Pic}^0(D) \\ \mathcal{D}_1, \mathcal{D}_2 & \mapsto & \mathcal{D}_1 + \mathcal{D}_2 - [\kappa_D] \end{array}$$

maps $F \times F$ into $\ker(\pi_*)$.

Depending on the type of Γ^-, this gives us different descriptions of $\mathrm{Prym}(D/C)$. The case numbering is in correspondence with Table 1.

Case 0: Γ^- is a double counting line. This case does not occur because assuming it does leads to a contradiction. By choosing coordinates appropriately, Γ^- is described by the equation $\lambda_1^2 = 0$. It follows that $Q_1^- + \lambda_2 Q_2^- + \lambda_3 Q_3^-$ is non-singular for all λ_2, λ_3. It follows that $Q_2^- = Q_3^- = 0$. Therefore, D has an intersection with $\{u = v = w = 0\}$ and thus ι would be ramified.

Case 2: Γ^- is a split singular conic, i.e., $L_1 \cup L_2$. In that situation, F consists of two components E_1 and E_2, covering L_1 and L_2 respectively. Each of these covers is ramified at a degree 4 locus: the intersection of L_i with the other components of Γ. Hence E_1 and E_2 are curves of genus 1. In fact, each has a rational point above $L_1 \cap L_2$, so we can identify them with their Jacobians. We have the map

$$\begin{array}{ccc} E_1 \times E_2 & \to & \mathrm{Jac}(D) \\ (\mathcal{D}_1, \mathcal{D}_2) & \mapsto & \mathcal{D}_1 + \mathcal{D}_2 - [\kappa_D] \end{array}.$$

Note that $(\mathcal{D}_1, \mathcal{D}_2)$ only map to 0 if $Q_{\mathcal{D}_1} = Q_{\mathcal{D}_2}$. This can only happen above the (ramified) point $L_1 \cap L_2$, so the map is an injection. Since $E_1 \times E_2$ is connected,

the image is contained in $\mathrm{Prym}(D/C)$ and because $E_1 \times E_2$ is an Abelian surface itself, we have equality:

$$\mathrm{Prym}(D/C) \cong E_1 \times E_2.$$

Case 3: Γ^- is a non-split singular conic. Then, over some quadratic extension $K(\sqrt{d})$ of K, the conic Γ^- splits and the analysis above applies. It follows that in that situation E_1 and E_2 are elliptic curves that are conjugate with respect to $K(\sqrt{d})/K$. By Weil-restriction, it follows that

$$\mathrm{Prym}(D/C) \cong \Re_{K(\sqrt{d})/K}(E_1).$$

Case 4: Γ^- is a non-singular conic. In that case, Q_1^-, Q_2^-, Q_3^- are K-linearly independent and therefore span the space of quadratic forms in r, s. Without loss of generality, we can assume

$$\begin{array}{rl} Q_1: & Q_1^+(u,v,w) = r^2, \\ Q_2: & Q_2^+(u,v,w) = rs, \\ Q_3: & Q_3^+(u,v,w) = s^2. \end{array}$$

It follows that Γ^- is given by the equation $4\lambda_1\lambda_3 = \lambda_2^2$ and we have a parametrisation

$$\begin{array}{ccc} \mathbb{P}^1 & \to & \Gamma^- \\ (x:1) & \mapsto & (1:2x:x^2). \end{array}$$

The curve F is a double cover of the Γ^-, ramified above $\Gamma^+ \cap \Gamma^-$. Using the parametrisation above we get an equation of the form

$$\det(Q_1^+ + 2xQ_2^+ + x^2Q_3^+) = \delta y^2.$$

for some $\delta \in K^*$. In order to determine the correct value of δ, suppose we have $\mathcal{D} \in F$ such that $2\mathcal{D} \neq [\kappa_D]$. Then $|\mathcal{D}|$ is cut out by a system of planes on Q. Supposing $\mathcal{D}$ is rational over K, the system of planes must be as well (but note that $|\mathcal{D}|$ itself does not need to contain rational divisors, nor does the system need to contain any planes rational over K). Using the parametrisation above, there is an $(x:1) \in \mathbb{P}^1(K)$ such that

$$Q^- = r^2 + 2xrs + x^2s^2.$$

It follows that $(0:0:0:x:-1)$ is the singular point of Q and that Q is a cone over the quadric in $\mathbb{P}^3$ given by

$$Q^+(u,v,w) - r^2 = 0.$$

According to Lemma 2.5, this quadric has two rational systems of lines (and therefore, a cone over it has two rational systems of planes) if

$$-\det Q^+ = -\det(Q_1^+ + 2xQ_2^+ + x^2Q_3^+)$$

is a square in K. It follows that F is isomorphic to

$$F: y^2 = -\det(Q_1^+ + 2xQ_2^+ + x^2Q_3^+).$$

The map $F \times F \to \mathrm{Pic}^0(D)$ described above gives rise to an isomorphism

$$\mathrm{Prym}(D/C) \simeq \mathrm{Jac}(F).$$

In Cases 2 and 3 above, the Jacobian of D contains elliptic curves E_1, E_2. In these cases, D is in fact a double cover of genus 1 curves C_1 and C_2 with $\mathrm{Jac}(C_i) \cong E_i$. The cover can be constructed explicitly in the following way. The $Q \in L_i$ have a

Case	C	D	Γ^-	$\mathrm{Prym}(D/C)$
1	Hyperelliptic	Hyperelliptic	—	$\mathrm{Jac}(F)$
2	Hyperelliptic	Non-hyperelliptic	split singular	$E_1 \times E_2$
3	Hyperelliptic	Non-hyperelliptic	non-split singular	$\Re_{K(\sqrt{d})/K}(E)$
4	Non-hyperelliptic	Non-hyperelliptic	non-singular	$\mathrm{Jac}(F)$

TABLE 1. Structure of the Prym variety

Case	Models
1	$C:\ \ y^2 = Q(x)R(x)$ where $\deg(Q) = 2, \deg(F) = 6$ $D:\ \ y_1^2 = Q(x)$ and $y_2^2 = R(x)$ $F:\ \ y_2^2 = R(x)$.
2	$C:\ \ y^2 = R_1(x)R_2(x)$ where $\deg(R_1) = \deg(R_2) = 4$ $D:\ \ y_1^2 = R_1(x)$ and $y_2^2 = R_2(x)$ $E_1:\ \ \mathrm{Jac}(y_1 = R_1(x))$ $E_2:\ \ \mathrm{Jac}(y_2 = R_2(x))$.
3	$C:\ \ y^2 = N_{K(\sqrt{d})[x]/K[x]}R(x)$ where $\deg(R) = 4$ $D:\ \ (x, y_0, y_1)$ satisfying $(y_0 + y_1\sqrt{d})^2 = R(x)$ $E:\ \ \mathrm{Jac}(y = R(x))$
4	$C:\ \ Q_1(u,v,w)Q_3(u,v,w) = Q_2(u,v,w)^2$ with Q_i quadratic forms $D:\ \ \begin{cases} Q_1(u,v,w) &= r^2 \\ Q_2(u,v,w) &= rs \\ Q_3(u,v,w) &= s^2 \end{cases}$ $F:\ \ y^2 = -\det(Q_1 + 2xQ_2 + x^2Q_3)$

TABLE 2. Models of involved curves

fixed singularity on the line $\{u = v = w = 0\}$. Projecting from that singularity yields an intersection of two quadrics in $\mathbb{P}^3$, a model of C_i. Let $\sigma_i \in \mathrm{Aut}_{\overline{K}}(D)$ denote the involution of D over E_i. We have $\iota = \sigma_1\sigma_2$. In fact, the projection $(u : v : w : r : s) \to (u : v : w)$ corresponds to $D \to D/\langle\sigma_1, \sigma_2\rangle$. This shows that the canonical model of C is in fact of genus 0 and hence that C is hyperelliptic. This places us in the situation of Section 2.2.

Theorem 5.1. *Let K be a field of characteristic 0 and let C be a curve of genus 3 over K with an unramified double cover D/C. Then $\mathrm{Prym}(D/C)$ can be described as given in Table 1 depending on the nature of C and D. Models of the curves involved can be described as in Table 2. For hyperelliptic curves, it is assumed they are hyperelliptic over a $\mathbb{P}^1$ over K.*

6. MAPPING D INTO $\mathrm{Prym}(D/C)$

As was shown in Section 5, if C is hyperelliptic then D is a cover of the curves that span $\mathrm{Prym}(D/C)$. Hence, it is obvious how to map D into $\mathrm{Prym}(D/C)$. In this section we show how D can be mapped into $\mathrm{Prym}(D/C)$ if C is non-hyperelliptic.

First, if we have a rational point $P_0 \in D(K)$, we can embed D in $\mathrm{Jac}(D)$ via the *Abel-Jacobi map*

$$\begin{array}{rcl} D & \to & \mathrm{Jac}(D) \\ P & \mapsto & [P - P_0]. \end{array}$$

When we combine this map with the projection map $(\mathrm{id}_* - \iota_*) : \mathrm{Jac}(D) \to \mathrm{Prym}(D/C)$, we obtain the *Abel-Prym map*

$$\begin{array}{rcc} D & \to & \mathrm{Prym}(D/C) \\ P & \mapsto & [P - \iota(P)] - [P_0 - \iota(P_0)]. \end{array}$$

In general, we do not have a rational base point P_0 at our disposal. We give an alternative map, based on the description of $\mathrm{Prym}(D/C)$ as $\mathrm{Jac}(F)$ for some component F of $W_4^1(D)$.

Let P_0 be a point on D and let L be the tangent line of C at $\pi(P)$. Then $L \cdot C$, being a linear section of a canonical model, determines an effective canonical divisor on C. Consequently, $\pi^*(L \cdot C) = 2P_0 + 2\iota(P_0) + P_1 + \iota(P_1) + P_2 + \iota(P_2)$ is an effective canonical divisor on D.

We use the notation from Section 3. Furthermore, we write $\mathrm{Tang}_D(P)$ for the tangent line of D at P and for a quadric $Q \subset \mathbb{P}^n$ and $P, T \in \mathbb{P}^n$ we write $P^t Q T$ for the matrix product, where Q is identified with its representing $(n+1) \times (n+1)$ symmetric matrix and P, T are interpreted as $(n+1)$-dimensional column vectors of projective coordinates.

Lemma 6.1. *With the notation as above, let P be a point in $D(\overline{K})$.*

(i) *There are two divisors $\mathfrak{D}_1, \mathfrak{D}_2$ (with $\mathfrak{D}_1 = \mathfrak{D}_2$ in degenerate cases) such that $\mathfrak{D}_i \geq 2P$ and $[\mathfrak{D}_i] \in F(\overline{K}) \subset W_4^1(\overline{K})$.*

(ii) *If $\mathfrak{D}_1 = 2P + P_1 + P_2$ then $\mathfrak{D}_2 = 2P + \iota(P_1) + \iota(P_2)$.*

(iii) *Let $T \in \mathrm{Tang}_D(P)$ with $T \neq P$. Then $x_*(\mathfrak{D}_i)$ satisfies*

$$(T^t \cdot Q_1 \cdot T) + 2x(T^t \cdot Q_2 \cdot T) + x^2(T^t \cdot Q_3 \cdot T) = 0.$$

(iv) *The map*

$$\begin{array}{rccc} \varphi : & D(\overline{K}) & \to & \mathrm{Div}^2(F/\overline{K}) \\ & P & \mapsto & [\mathfrak{D}_1] + [\mathfrak{D}_2] \end{array}$$

is defined over K.

Proof. (iii): By Lemma 4.1 we have that if $\mathfrak{D} \in F$ with $\mathfrak{D} = 2P + P_1 + P_2$, then $\mathrm{Tang}_D(2P) \subset V_{\mathfrak{D}} \subset Q_{\mathfrak{D}}$. This is exactly the case if $T \in Q_{\mathfrak{D}}$ for some (and hence for all) $T \in \mathrm{Tang}_D(P)$ with $T \neq P$. Using that $\Gamma^- \simeq \mathbb{P}^1$ via $(1 : 2x : x^2) \mapsto (x : 1)$, we get the desired equation.

(i): From (iii), we know that there are two quadrics $Q \in \Gamma^-$ containing $\mathrm{Tang}_D(P)$. We show that such a conic is $Q_{\mathfrak{D}}$ for some $\mathfrak{D} \in F$ such that $\mathfrak{D} \geq 2P$. Consider the plane V spanned by $\mathrm{Tang}_D(P)$ and a singular point $(0 : 0 : 0 : x : -1)$ of Q. Then $V \subset Q$ and by Lemma 4.1, $\mathfrak{D} = V \cdot D$ represents a divisor class in $W_4^1(D)$ and $Q = Q_{\mathfrak{D}}$.

If there is another divisor $\mathfrak{D}' \geq 2P$ with $Q_{\mathfrak{D}'} = Q$, then $\mathfrak{D} - \mathfrak{D}'$ or $\mathfrak{D} - \iota_*(\mathfrak{D}')$ is principal. Taking the image under π_* would give a divisor of a degree 2 function on C, which contradicts that C is not hyperelliptic.

(ii): Note that $\pi_*(\mathfrak{D}_2) = \pi_*(\mathfrak{D}_1) = C \cdot \mathrm{Tang}_C(\pi(P))$. If $\mathfrak{D}_2 = 2P + P_1 + \iota(P_2)$ then $2P + P_1$ must lie on the line $V_{\mathfrak{D}_1} \cap V_{\mathfrak{D}_2}$. Since D is canonical, it follows that $l(2P + P_1) = 2$. This contradicts Lemma 3.1. It follows that $\mathfrak{D}_2$ must be as stated.

(iv): Verify that ${}^{\sigma}(\varphi(P)) = \varphi({}^{\sigma}P)$ for $\sigma \in \mathrm{Gal}(\overline{K}/K)$ via direct computation. $\square$

Proposition 6.2. *Let C be a non-hyperelliptic genus 3 curve over a field K of characteristic 0 and let D/C be an unramified double cover with $\iota : D \to D$ the associated involution. Let F be the genus 2 curve given by Theorem 5.1 such that $\mathrm{Jac}(F) = \mathrm{Prym}(D/C)$ and let $\varphi : D \to \mathrm{Div}^2(F)$ be the map defined in Lemma 6.1. Then we have*

$$\begin{array}{rccc} 2(\iota_* - \mathrm{id}_*) : & D(\overline{K}) & \to & \mathrm{Prym}(D/C)(\overline{K}) \\ & P & \mapsto & [\varphi(P) - \kappa_F]. \end{array}$$

Proof. Using (ii) of Lemma 6.1, we have $\varphi(P) = 4P + P_1 + P_2 + \iota(P_1) + \iota(P_2)$. Using that $[\kappa_D] = [2P + 2\iota(P) + P_1 + P_2 + \iota(P_1) + \iota(P_2)]$, we have $[\varphi(P) - \kappa_D] = 2P - 2\iota(P)$ as an element of $\mathrm{Pic}(D)$. Note that $[\kappa_D] = [\mathfrak{D} + \iota(\mathfrak{D})]$ for any $[\mathfrak{D}] \in F \subset W_4^1(D)$, so identifying $\mathrm{Pic}(F) \subset \mathrm{Pic}(D)$, we get $[\kappa_F] = [\kappa_D]$. This proves the proposition. □

Remark 6.3. It is worth noting that the map $(\iota_* - \mathrm{id}_*) : D \to \ker(\pi_*)$ does not map D to $\mathrm{Prym}(D/C)$. To see this, note that $\mathrm{Prym}(D/C) = \mathrm{Jac}(F)$ for some genus 2 curve F. Any degree 0 divisor class on F can be represented as the difference of two points on F, so we have that $\mathrm{Prym}(D/C) = F - F$. If $P \in D(\overline{K})$ has $[\iota(P) - P] \in \mathrm{Prym}(D/C)$, then we can find $[\mathfrak{D}_1], [\mathfrak{D}_2] \in F(\overline{K})$ such that $[\iota(P) - P] = [\mathfrak{D}_1 - \mathfrak{D}_2]$. Since $F \subset W_4^1(D)$, we can choose effective representatives $\mathfrak{D}_1, \mathfrak{D}_2$ with a given point in the support. Hence, we can assume that $\mathfrak{D}_1 = \iota(P) + P_2 + P_3 + P_4$ and $\mathfrak{D}_2 = P + P_5 + P_6 + P_7$. It follows that $0 = [P_2 + P_3 + P_4 - P_5 - P_6 - P_7]$, so ι has a fixed point or D is hyperelliptic or trigonal. Our assumptions and Lemma 3.1 tell us that none of these are the case.

Lemma 6.1 together with Proposition 6.2 provide an explicit way of mapping D into an Abelian surface $\mathrm{Prym}(D/C) \simeq \mathrm{Jac}(F)$. By slight abuse of notation, we write $\varphi : D \to \mathrm{Jac}(F)$.

For explicit computations, Abelian surfaces have proven to be rather unwieldy. In many cases, enough of the variety structure remains in the associated Kummer-surface $\mathcal{K} = \mathrm{Jac}(F)/\langle -1 \rangle$. The surface $\mathcal{K}$ is naturally expressed as a quartic surface in $\mathbb{P}^3$. The map

$$\begin{array}{lcccc} k : & \mathrm{Jac}(F) & \to & \mathcal{K} & \\ & [(x_1, y_1) + (x_2, y_2) - \kappa_F] & \mapsto & (1 : x_1 + x_2 : x_1 x_2 : \ldots) & = (k_1 : k_2 : k_3 : k_4) \end{array}$$

expresses $\mathrm{Jac}(F)$ as a double cover of $\mathcal{K}$, ramified at $\mathrm{Jac}(F)[2]$, which maps to the singular locus of $\mathcal{K}$. The equation of $\mathcal{K}$ is of the form

$$\mathcal{K} : (k_2^2 - 4k_1 k_3) k_4^2 + K_3(k_1, k_2, k_3) k_4 + K_4(k_1, k_2, k_3) = 0,$$

where K_3, K_4 are homogeneous forms of degrees $3, 4$ respectively (see [8] for explicit formulae). Hence, $\mathcal{K}$ is itself a double cover of the projective plane with coordinates $(k_1 : k_2 : k_3)$ outside the point $(0 : 0 : 0 : 1)$.

Since $\iota_* \circ 2(\iota_* - \mathrm{id}_*) = -1 \circ 2(\iota_* - \mathrm{id}_*)$, we see that $D \to k\varphi(D)$ factors through $D/\langle \iota \rangle = C$. Furthermore, if $\mathfrak{D} \in \mathrm{Div}^2(F)$ is effective and $(k_1 : k_2 : k_3 : k_4) = k([\mathfrak{D} - \kappa_F])$, then $x_*(\mathfrak{D})$ satisfies

$$k_3 - k_2 x + k_1 x^2 = 0.$$

This gives us a procedure to compute many pointwise images for $k\varphi$:

(1) Choose an extension L and a point $P \in D(L)$ (since D is given as a degree 8 curve, there is an abundance of suitable degree 8 extensions)

(2) Following Lemma 6.1, choose $T \in \mathrm{Tang}_D(P)$ and set

$$(k_1, k_2, k_3) = (T^t \cdot Q_1 \cdot T, -2T^t \cdot Q_2 \cdot T, T^t \cdot Q_3 \cdot T)$$

(3) If $k_3 - k_2x + k_1x^2$ is irreducible of degree 2 over L, then there is a unique point $(k_1 : k_2 : k_3 : k_4) \in \mathcal{K}(L)$ that has an L-rational preimage in $\mathrm{Jac}(F)$. This is the desired image.

The irreducibility in the last step corresponds to P_1, P_2 from Lemma 6.1(ii) being quadratic conjugate over L. In that case, the divisor $P_1 + \iota(P_2)$ is not L-rational and hence rationality tells which divisor to pick. If P_1, P_2 are themselves L-rational, then the above procedure does not compute sufficient information to distinguish between $2P + P_1 + P_2$ and $P + \iota(P) + P_1 + \iota(P_2)$.

The procedure above yields a way to compute the equations of $k\varphi(D)$. First, one gathers many pointwise images for points over extensions L and then one interpolates for low degree rational forms vanishing on those points. As we will see, $k\varphi(D)$ is the intersection of $\mathcal{K}$ with another degree 4 surface.

Lemma 6.4. *With the notation above, the image of D under $k \circ \varphi$ is of degree at most* 16*.*

Proof. We compute the degree of the image by computing the degree of the intersection with $k_1 = 0$. By change of basis we can assume that Q_3 is of rank 4. A point $P \in D$ has $k_1 = 0$ if Q_3 contains the plane $V_{\mathfrak{D}}$ for some $\mathfrak{D} \geq 2P$. The two plane rulings on Q_3 give rise to two degree 4 covers $D \to \mathbb{P}^1$, where the fibres are the divisors cut out by the $V_{\mathfrak{D}}$ in the ruling. From Riemann-Hurwitz it follows that for each ruling there are 16 ramified fibres, i.e., $\mathfrak{D}$ of the form $2P + P_1 + P_2$. Hence, we see that there are 32 points on D (counted with appropriate multiplicity) that land on $k_1 = 0$. Note that the image of D under $k\varphi$ factors through $D/\langle\iota\rangle$, so the degree of $k\varphi(D)$ is at most 16. □

The procedure above has been implemented as a routine for the computer algebra system MAGMA [2]. See [6].

7. The fibre of the Prym map in genus 3

Given a genus 2 curve F, we have an Abelian variety $\mathrm{Jac}(F)$ and a quartic surface $\mathrm{Jac}(F)/\langle -1 \rangle = \mathcal{K} \subset \mathbb{P}^3$, with a singular locus consisting of the image of $\mathrm{Jac}(F)[2]$. There is an obvious way of realising $\mathrm{Jac}(F)$ as a Prym variety of a non-hyperelliptic curve of genus 3. Pick a plane $V \subset \mathbb{P}^3$ such that $C := V \cap \mathcal{K}$ is a non-singular quartic curve. It follows that C stays away from the singular points of $\mathcal{K}$ and thus does not meet the ramification locus of $k : \mathrm{Jac}(F) \to \mathcal{K}$. Therefore $D = k^{-1}(C)$ is an unramified cover of C. Either D is connected and hence of genus 5 or D is the disjoint union of two copies of C. Note however that C is of genus 3 and hence has to be special to fit in an Abelian surface.

In fact, as Verra [24] proves, over an algebraically closed field, essentially any occurrence of $\mathrm{Jac}(F)$ as $\mathrm{Prym}(D/C)$ occurs for C isomorphic to a linear section of $\mathcal{K}$. The addition of $\mathrm{Jac}(F)[2]$ induces automorphisms of $\mathcal{K}$ which are induced by linear transformations of $\mathbb{P}^3$. He shows that the fibre of the Prym map $(D/C) \mapsto \mathrm{Prym}(D/C)$ over $\mathrm{Jac}(F)$ is a blow-up of $\widehat{\mathbb{P}}^3/\mathrm{Jac}(F)[2]$, where $\widehat{\mathbb{P}}^3$ is the space of plane sections of $\mathcal{K}$.

Verra also proves that genus 5 curves $D \subset \mathrm{Jac}(F)$ of the form above are, up to translation by a 2-torsion point, Abel-Prym embeddings. We give a short description of a procedure to recover

$$C : Q_1(u,v,w)Q_3(u,v,w) = Q_2(u,v,w)^2$$

from a plane section of the Kummer surface $\mathcal{K} = \mathrm{Jac}(F)/\langle -1\rangle$ for a curve F of genus 2.

First we review some of the basic geometry of Jacobians of curves of genus 2. We follow the notation introduced in [8]. Let F be a curve of genus 2. They define a projective model of $\mathrm{Jac}(F)$ in $\mathbb{P}^{15}$ with coordinates $(z_0 : \cdots : z_{15})$ with (among others) the following properties:

- There is a symmetric theta-divisor Θ on $\mathrm{Jac}(F)$ such that
$$\langle k_1, \ldots, k_4\rangle = |2\Theta|$$
and
$$\langle z_0, \ldots, z_{15}\rangle = |4\Theta|$$
with
$$(k_1 : k_2 : k_3 : k_4) = (z_{14} : z_{13} : z_{12} : z_5).$$
- The coordinates $(k_1 : k_2 : k_3 : k_4)$ provide a model of the Kummer surface $\mathcal{K} = \mathrm{Jac}(F)/\langle -1\rangle$.
- With respect to the action of $-1 \in \mathrm{Aut}(\mathrm{Jac}(F))$ on $|4\Theta|$, we have that
$$\langle z_0, z_3, z_4, z_5, z_{10}, \ldots, z_{15}\rangle = \langle k_1^2, k_1k_2, \ldots, k_4^2\rangle$$
is the $+1$-eigenspace and
$$\langle g_0, \ldots, g_5\rangle := \langle z_1, z_2, z_6, z_7, z_8, z_9\rangle$$
is the -1-eigenspace.

Let $V = \{k_4 = v_1k_1 + v_2k_2 + v_3k_3\} \subset \mathbb{P}^3$ be a plane such that $C = \mathcal{K} \cap V$ is a non-singular plane section and let $(u : v : w) = (k_1 : k_2 : k_3)$ be coordinates on V (since $(0 : 0 : 0 : 1)$ is a singular point of $\mathcal{K}$, assuming the suggested form of V is not a restriction). The curve C is a nonsingular degree 4 plane curve. It follows that C is of genus 3 and that $(u : v : w)$ gives a canonical model of C, i.e., that $\langle u|_C, v|_C, w|_C\rangle = |\kappa_C|$ for some canonical divisor κ_C of C. Let D be as above and let κ_D be the pull-back of κ_C. It is a straightforward computation to check that the restriction of $\langle z_0, \ldots, z_{15}\rangle$ to D gives a linear system contained in $|\kappa_D|$ and that generically it gives the complete linear system.

Using the quadratic relations between the z_i (see [15], [8] and [14] for the explicit formulae), we can express any g_ig_j as a degree 4 form in $k_1, \ldots, k_4$. Hence, we obtain that

$$(a_0g_0 + \cdots + a_5g_5)^2 = G(a_0, \ldots, a_5; k_1, \ldots, k_4),$$

where G is homogeneous of degrees $2, 4$ in the a_i and the k_j respectively.

Insisting that

$$G(a_0, \ldots, a_5) = u^2Q(u,v,w)$$

for some quadratic form Q gives 9 quadratic equations in $a_0, \ldots, a_5$. However, a solution to these equations corresponds exactly to a form $Q(u,v,w)$ on C that becomes a square when pulled back to D. We know that this happens for exactly two forms $Q_1^+(u,v,w) = r^2$ and $Q_3^+(u,v,w) = s^2$, so these equations determine a degree 2 locus in $(a_0 : \cdots : a_5)$.

Solving these equations allows us to determine $Q_1^+(u,v,w)$ and $Q_3^+(u,v,w)$ up to a scalar. The quadratic form $Q_2^+(u,v,w)$ is then easily determined up to a scalar because this corresponds to the conic through the intersection of $Q_1^+(u,v,w)Q_3^+(u,v,w) = 0$ with C. The appropriate scalars λ, μ are then easily determined from the fact that

$$\lambda Q_1^+(u,v,w)\mu Q_3^+(u,v,w) - (\mu Q_2^+(u,v,w))^2$$

should equal the equation for C.

Note that we may find Q_i^+ that are quadratic conjugate over the base field we are working with, because of the arbitrary coordinate choice we made when insisting that $G = u^2 Q(u,v,w)$. The analysis from Section 3 guarantees us that by change of basis (corresponding to $\mathrm{Aut}(\Gamma^-)$ or, equivalently, fractional linear transformations of x) we can in fact obtain rational Q_1^+, Q_3^+. This yields the following amusing result, which is equivalent to saying that all Jacobians of genus 2 curves over $\mathbb{Q}$ occur as Prym varieties of non-hyperelliptic curves of genus 3 over $\mathbb{Q}$.

Proof of Proposition 1.3: Take the curve of genus 2

$$F : y^2 = f(x)$$

and take a sufficiently general plane section of the associated Kummer-surface. Using the construction above, we obtain a cover $D \to C$ such that $\mathrm{Prym}(D/C) = \mathrm{Jac}(F)$. Section 3 tells us that F must be of the described form and the outline above explains how one can find the representation explicitly. $\square$

In fact, the model of C as a plane section of a Kummer-surface $\mathcal{K}$ completely encodes the 28 bitangents of C as well. The 16 tropes of $\mathcal{K}$ obviously cut out bitangents on C. The remaining 12 bitangents come in pairs, making up the 6 singular conics in the family $Q_1^+ + 2xQ_2^+ + x^2Q_3^2$.

This gives us a way to search for genus 3 curves with all bitangents rational. First, start with a Kummer-surface $\mathcal{K}$ with 16 rational tropes (i.e., the Kummer-surface of the Jacobian of a genus 2 curve with 6 rational Weierstraß points). Then, select a plane V such that $C := V \cap \mathcal{K}$ is of the form

$$Q_1^+(u,v,w)Q_3^+(u,v,w) = Q_2^+(u,v,w)^2,$$

where the singular conics in $Q_1^+ + 2xQ_2^+ + x^2Q_3^2$ are split. As it turns out, these are all split or nonsplit simultaneously.

Example: *A curve of genus* 3 *with all* 28 *bitangents rational.*

Take

$$F : y^2 = x(x-2)(x-1)(x+1)(x+3).$$

The corresponding Kummer-surface is

$$\begin{aligned}\mathcal{K} : 36k_1^4 + 84k_1^3k_3 - 24k_1^2k_2k_3 - 12k_1^2k_2k_4 + 65k_1^2k_3^2 + 4k_1^2k_3k_4 - 24k_1k_2^2k_3 + \\ 4k_1k_2k_3^2 + 14k_1k_2k_3k_4 + 14k_1k_3^3 - 4k_1k_3^2k_4 - 4k_1k_3k_4^2 + k_2^2k_4^2 - 2k_2k_3^2k_4 + k_3^4 = 0.\end{aligned}$$

We take the plane section

$$V : k_1 + k_2 + tk_3 + k_4 = 0.$$

Projecting onto $(u : v : w) = (k_1 : k_2 : k_3)$, we obtain

$$C : Q_1^+(u,v,w)Q_3^+(u,v,w) = Q_2^+(u,v,w)^2$$

where

$$\begin{aligned} Q_1^+ &= (36t-82)u^2+(6t-80)uv+(-11t+14)uw+(6t+2)v^2+\\ &\quad (t+14)vw+tw^2,\\ Q_2^+ &= (-3t+40)u^2+(-\tfrac{1}{2}t-9)uv+(-6t^2+\tfrac{11}{2}t+51)uw+\\ &\quad (-\tfrac{1}{2}t-7)v^2+(-\tfrac{1}{2}t^2-2t+2)vw+(-t^2+\tfrac{1}{2}t+7)w^2,\\ Q_3^+ &= (6t+2)u^2+(t+14)uv+(t^2+2t-4)uw+tv^2+(2t^2-t-14)vw+\\ &\quad (t^3-t^2-8t+2)w^2. \end{aligned}$$

The 16 bitangents coming from the tropes are given by the polynomials

$$\begin{aligned} &u,\ w,\ 4u-2v+w,\ 5u+3v+(t+1)w,\ 4u+v+(t+2)w,\ u+7v+(t-1)w,\\ &u-v+w,\ 7u+v+(-t-3)w,\ 9u+3v+w,\ 7u+v+(t+1)w,\\ &5u-v+(-t+1)w,\ u-v+(-t+3)w,\ 2u-4v+(-t+2)w,\\ &10u-2v+(t-4)w,\ u+v+w,\ 2u+2v+tw. \end{aligned}$$

The remaining 12 bitangents come from the 6 singular quadrics. They are split if $196+20t-23t^2$ is a square. Therefore, we substitute

$$t := \frac{4s^2-10s-6}{2s^2+s+3}$$

and obtain the bitangents given by the polynomials

$$\begin{aligned} &(s+21)u+(7s+3)v+(s-3)w,\ (10s+11)u+(-2s+5)v+(-2s-1)w,\\ &(8s^3+2s^2+11s-3)u+(2s^3+5s^2+5s+6)v+(8s^3+17s^2-s-6)w,\\ &(10s^3-s^2+12s-9)u+(-2s^3-7s^2-6s-9)v+(-2s^3+5s^2+30s-9)w,\\ &(4s^3+4s^2+7s+3)u+(2s^2+s+3)v+(2s^2+3s-3)w,\\ &(2s^3-5s^2-9)u+(-2s^3-3s^2-4s-3)v+(2s^3+7s^2+4s-1)w,\\ &(2s^3+7s^2+6s+9)u+(2s^3+s^2+3s)v+(2s^3+s^2-3s)w,\\ &(4s^3+10s^2+10s+12)u+(-2s^3+s^2-2s+3)v+(s^3+4s^2-5s)w,\\ &(4s^3+16s^2+13s+21)u+(-4s^3-5s+3)v+(4s^3+16s^2-3s-3)w,\\ &(10s^3+23s^2+24s+27)u+(6s^3+s^2+8s-3)v+(6s^3-5s^2-20s+7)w,\\ &(14s^3+13s^2+24s+9)u+(2s^3-5s^2-9)v+(-10s^3-35s^2+9)w,\\ &(4s^3-8s^2+s-15)u+(4s^3+4s^2+7s+3)v+(4s^3-8s^2-23s+9)w. \end{aligned}$$

8. Applications to finding rational points on curves of genus 3

In this section, we will apply the concepts of *covering collections* (see [10], [25], [4], [7]) and *Chabauty methods* (see [11], [16]) to a curve C of genus 3 with an unramified double cover D. We end up determining the rational points on a curve of genus 5 inside the Jacobian of a curve F of genus 2. The hardest piece of information we will need is the Mordell-Weil group of $\mathrm{Jac}(F)$. Computationally, this is much more attractive than applying Chabauty methods directly to an embedding of C in its own Jacobian. In the latter case, we would have to analyse the Mordell-Weil group of $\mathrm{Jac}(C)$.

Additionally, the techniques we present here do not depend on the existence of an embedding of C in $\mathrm{Jac}(C)$. As a result, we will see that we can even use the construction to exhibit part of a local-global obstruction for C and D having rational points.

Let K be a number field and let C be a non-hyperelliptic curve of genus 3 with an unramified double cover D over K. As we have seen in Section 3, it follows that there exists a smooth plane model of C of the form

$$Q_1(u,v,w)Q_3(u,v,w) = Q_2(u,v,w)^2,$$

where $Q_1, Q_2, Q_3 \in K[u, v, w]$ are quadratic forms. Without loss of generality, we can assume that Q_1, Q_2, Q_3 have integral coefficients. Furthermore, we have a collection of twists of D, each covering C, of the form:

$$D_\delta : \begin{cases} Q_1(u, v, w) = \delta r^2 \\ Q_2(u, v, w) = \delta rs \\ Q_3(u, v, w) = \delta s^2 \end{cases}$$

We write $\mathcal{O} = \mathcal{O}_K$ for the ring of integer of K and we consider the projective $\mathcal{O}_K$-scheme X corresponding to the ideal $I = (Q_1, Q_3, Q_1Q_3 - Q_2^2)\mathcal{O}_K[u, v, w]$. Since C is non-singular as a curve over K, we have that $X \times_{\mathcal{O}_K} \mathrm{Spec}(K)$ is empty. Let S be a finite set of primes such that $X \times \mathrm{Spec}(\mathcal{O}_S)$ is empty. Such a set S is easily computed. For instance, compute

$$\mathrm{Res}_u(\mathrm{Res}_v(Q_1, Q_3), \mathrm{Res}_v(Q_1, Q_2)) = \lambda w^{16}.$$

One can take S to be the set of prime divisors of λ. One may obtain a smaller set by intersecting such sets S obtained from all different combinations in which such resultants could be taken. We recall the definition

$$K(S, 2) := \{\delta \in K^* : v_\mathfrak{p}(\delta) \equiv 0 \mod 2 \text{ for all primes of } K \text{ satisfying } \mathfrak{p} \notin S\}/K^{*2}.$$

This is a finite subgroup of K^*/K^{*2} and we will identify its elements with a finite set of representatives in K^*.

We obtain the standard lemma:

Lemma 8.1. *Let C and Q_1, Q_2, Q_3 and S be as above. If $(u_0 : v_0 : w_0) \in C(K)$, then there exists $\delta \in K(S, 2)$ and $r_0, s_0 \in K$ such that*

$$(u_0 : v_0 : w_0 : r_0 : s_0) \in D_\delta(K).$$

It follows that any rational point on C has a rational pre-image on D_δ for some $\delta \in K(S, 2)$. Thus, in order to determine the rational points of C, it suffices to determine the rational points of D_δ for all $\delta \in K(S, 2)$. From Section 4 we know that for

$$F_\delta : y^2 = -\delta \det(Q_1 + 2xQ_2 + x^2Q_3),$$

we have $\mathrm{Prym}(D_\delta/C) \simeq \mathrm{Jac}(F_\delta)$ and Proposition 6.2 gives an explicitly computable map $\varphi : D_\delta \to \mathrm{Jac}(F_\delta)$. We can then proceed to determine $\varphi(D_\delta(\mathbb{Q})) \cap \mathrm{Jac}(F_\delta)(\mathbb{Q})$ or rather, as it turns out, $k(\mathrm{Jac}(F_\delta)(\mathbb{Q})) \cap k\varphi(D_\delta)(\mathbb{Q})$.

Example: *Chabauty using Prym varieties.*

Proof of Proposition 1.1: See [6] for a transcript of the computer calculations. Applying the method described above we verify that we can take $S = \{1, 2, 5\}$ and local considerations show that $D_\delta(\mathbb{Q}) = \emptyset$ for $\delta \neq -1$. We find

$$F : y^2 = x^5 + 8x^4 - 7x^3 - \frac{7}{2}x^2 + 5x - 1$$

and

$$\mathrm{Jac}(F)(\mathbb{Q}) = \langle \mathcal{D} \rangle = \langle [(2\sqrt{2} - 2, 17\sqrt{2} - 25) + (-2\sqrt{2} - 2, -17\sqrt{2} - 25) - 2\infty] \rangle.$$

The equation of the associated Kummer-surface is

$$\begin{aligned} \mathcal{K} : \quad & 11k_1^4 - 28k_1^3k_2 + 70k_1^3k_3 + 4k_1^3k_4 + 32k_1^2k_2^2 - 164k_1^2k_2k_3 - 10k_1^2k_2k_4 + 171k_1^2k_3^2 + \\ & 14k_1^2k_3k_4 + 4k_1k_2^3 - 20k_1k_2^2k_3 + 14k_1k_2k_3^2 + 14k_1k_2k_3k_4 + 14k_1k_3^3 - 32k_1k_3^2k_4 - \\ & 4k_1k_3k_4^2 + k_2^2k_4^2 - 2k_2k_3^2k_4 + k_3^4 = 0 \end{aligned}$$

and, using the interpolation procedure described in Section 6, we find that the embedding of C in $\mathcal{K}$ as $k\varphi(D)$ is given by the equation

$$\begin{aligned}\psi:\quad & 429136k_1^4 + 1330784k_1^3k_3 + 567232k_1^3k_4 - 159200k_1^2k_2^2 - 2866016k_1^2k_2k_3 + 33440k_1^2k_2k_4 + 4248768k_1^2k_3^2 + \\ & 27552k_1^2k_3k_4 + 881664k_1^2k_4^2 + 288072k_1k_2^3 - 777432k_1k_2^2k_3 - 256928k_1k_2^2k_4 + 244832k_1k_2k_3^2 + \\ & 907424k_1k_2k_3k_4 - 745472k_1k_2k_4^2 + 593152k_1k_3^3 - 991488k_1k_3^2k_4 + 357440k_1k_3k_4^2 + 573440k_1k_4^3 + 34895k_2^4 - \\ & 69720k_2^3k_3 + 1120k_2^3k_4 + 151704k_2^2k_3^2 - 364448k_2^2k_3k_4 + 226032k_2^2k_4^2 - 251552k_2k_3^3 + 569376k_2k_3^2k_4 + \\ & 10752k_2k_3k_4^2 - 315392k_2k_4^3 + 156704k_3^4 - 167552k_3^3k_4 - 283136k_3^2k_4^2 + 200704k_3k_4^3 + 114688k_4^4 = 0.\end{aligned}$$

It is a straightforward computation to check that the intersection of $\mathcal{K}$ with $\psi(k) = 0$ is non-singular, which verifies that $k\varphi(D)$ is indeed an embedding of C in $\mathcal{K}$ and that $\varphi(D)$ is an embedding of D in $\mathrm{Jac}(F)$.

Using that $\varphi : D \to \mathrm{Jac}(F)$ is defined over $\mathbb{Q}$ and that $\mathrm{Jac}(F)(\mathbb{Q}) = \langle \mathcal{D} \rangle$, we find that a rational point $P \in \varphi(D)(\mathbb{Q})$ must be of the form $P = n\mathcal{D}$ for some $n \in \mathbb{Z}$. Furthermore, considering the F and $\mathcal{K}$ over $\mathbb{F}_{13}$, we find that any such point must have $n \equiv \pm 1 \mod 10$.

Using the formal group law of $\mathrm{Jac}(F)$, we obtain a power series

$$\psi(N) = \psi(k((1 + 10N)\mathcal{D})) = \psi(K(\mathcal{D} + \mathrm{Exp}(N\mathrm{Log}(10\mathcal{D})))),$$

say,

$$\psi(N) = \psi_0 + \psi_1 N + \psi_2 N^2 + \cdots \in \mathbb{Z}_{13}[\![N]\!],$$

with $\psi_i \equiv 0 \mod 13^i$. such that, if $P = (1 + 10N)\mathcal{D}$ is a point on $\varphi(D)(K)$, then $\psi(N) = 0$.

Note that the values of $\psi(k(\mathcal{D})), \psi(k(11\mathcal{D}))$ determine $\psi_0, \psi_1 \mod 13^2$, so one does not need an explicit description of the formal group law on $\mathrm{Jac}(F)$ to obtain an approximation to $\psi(N)$.

Since $\psi(k(\mathcal{D})) = 0$ and $\psi(k(11\mathcal{D})) \not\equiv 0 \mod 13^2$, it follows that $\psi_1 \not\equiv 0 \mod 13^2$. From Straßmann's lemma it follows that $\psi(N)$ has at most one 0 for $N \in \mathbb{Z}_{13}$ (i.e., $N = 0$). This implies that $\varphi(D)$ has only one rational point which reduces to $\mathcal{D}$ modulo 13. By symmetry, it follows that there is also only one rational point reducing to $-\mathcal{D}$ modulo 13. On the other hand, the computation over $\mathbb{F}_{13}$ shows that all rational points of $\varphi(D)$ reduce to $\pm\mathcal{D}$ modulo 13. Hence, it follows that

$$\varphi(D)(K) = \{\mathcal{D}, -\mathcal{D}\}$$

and that C has only one rational point, being $(0 : 1 : 0)$. □

Example: *Computations in the Brauer-Manin obstruction.*

Since the embedding of D in $\mathrm{Prym}(D/C)$ is independent of D having any rational points, we can also apply this construction to curves D that have no rational points, but do have rational points everywhere locally. Using information obtained from the reduction of $\mathrm{Jac}(F)$ at various primes, we might actually succeed in *proving* that $D(\mathbb{Q})$ is empty. Under the assumption that $\mathrm{Jac}(D)$ has a finite Tate-Shafarevich group, this corresponds to computing part of the Brauer-Manin obstruction according to [22].

We consider the curve

$$C : (v^2 + vw - w^2)(uv + w^2) = (u^2 - v^2 - w^2)^2.$$

It is easily checked that C has points everywhere locally. Furthermore, the set of primes S described above can be taken to be $\{2\}$ and only for $\delta = 1$ does D_δ have points everywhere locally.

Proof of Proposition 1.2: See [6] for a transcript of the computer calculations. The fact that $D(\mathbb{Q}_p)$ and $D(\mathbb{R})$ are all non-empty can be verified with a straightforward

computation. To prove that $D(\mathbb{Q}) = \emptyset$ we embed D in $\mathrm{Prym}(D/C) = \mathrm{Jac}(F)$, where

$$F : y^2 = x^6 + 2x^5 + 15x^4 + 40x^3 - 10x.$$

We find that

$$\mathrm{Jac}(F)(\mathbb{Q}) = \langle \mathcal{D}_1, \mathcal{D}_2 \rangle \simeq \mathbb{Z} \times \mathbb{Z},$$

where

$$\begin{array}{rcl} \mathcal{D}_1 & = & [\infty^+ - \infty^-], \\ \mathcal{D}_2 & = & [\{x^2 + \frac{2}{5}x + \frac{1}{41} = 0, y = \frac{4683}{2050}x - \frac{281}{410}\} \cdot F - \kappa_F]. \end{array}$$

Considering $\mathrm{Jac}(F)$ modulo 7, we find

$$\varphi(D)(\mathbb{Q}) \subset \{\pm 9\mathcal{D}_1, \pm 22\mathcal{D}_1, \pm 23\mathcal{D}_1\} + \langle 55\mathcal{D}_1, \mathcal{D}_2 - 15\mathcal{D}_1 \rangle$$

and considering $\mathrm{Jac}(F)$ modulo 11, we find

$$\varphi(D)(\mathbb{Q}) \subset \{\pm 33\mathcal{D}_1\} + \langle 93\mathcal{D}_1, \mathcal{D}_2 + 46\mathcal{D}_1 \rangle.$$

Considering $\mathrm{Jac}(F)$ modulo 11^2, we find that the two residue classes modulo 11 lift to 11 residue class modulo

$$\langle 11 \cdot 93\mathcal{D}_1, 11 \cdot (\mathcal{D}_2 + 46\mathcal{D}_1) \rangle.$$

We combine the information modulo 11^2 and 7 and express it as congruences modulo

$$\langle 55\mathcal{D}_1, \mathcal{D}_2 - 15\mathcal{D}_1, 11 \cdot 93\mathcal{D}_1, 11 \cdot (\mathcal{D}_2 + 46\mathcal{D}_1) \rangle = \langle 11\mathcal{D}_1, \mathcal{D}_2 - 4\mathcal{D}_1 \rangle.$$

We obtain

$$\begin{array}{lcccccc} \text{from } 7 & : & \varphi(D)(\mathbb{Q}) & \subset & \{0, \pm\mathcal{D}_1, \pm 2\mathcal{D}_1\} & + & \langle 11\mathcal{D}_1, \mathcal{D}_2 - 4\mathcal{D}_1 \rangle \\ \text{from } 11^2 & : & \varphi(D)(\mathbb{Q}) & \subset & \{\pm 4\mathcal{D}_1\} & + & \langle 11\mathcal{D}_1, \mathcal{D}_2 - 4\mathcal{D}_1 \rangle \end{array}.$$

It follows that $D(\mathbb{Q}) = \emptyset$. and therefore that $C(\mathbb{Q})$ is empty as well. □

9. Acknowledgements

I would like to thank MSRI for their 2000 fall special semester on explicit methods in number theory for bringing me into contact with many mathematicians. I have greatly benefitted from the discussions I had with them. In particular I would like to thank, Armand Brumer, J. Merriman, Ed Schaefer, Michael Stoll and Joe Wetherell.

References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I*, volume 267 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1985.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] N. Bruin and E. V. Flynn. n-covers of hyperelliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 134(3):397–405, 2003.

[4] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[5] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[6] Nils Bruin. Routines and transcript of computations. available from `http://www.cecm.sfu.ca/~ bruin/g3prym`, 2004.

[7] Nils Bruin and E. Victor Flynn. Towers of 2-covers of hyperelliptic curves. Technical Report PIMS-01-12, PIMS, 2001. `http://www.pims.math.ca/publications/#preprints`.

[8] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. LMS–LNS 230. Cambridge University Press, Cambridge, 1996.
[9] A Cayley. On the bitangents of a quartic. In *A treatise on the higher plane curves*, pages 387–389. Chelsea, New York, 1879.
[10] C. Chevalley and A. Weil. Un théorème d'arithmétiques sur les courbes algébriques. *C.R.*, 195:570–572, 1930.
[11] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.
[12] Ron Donagi. The fibers of the Prym map. In *Curves, Jacobians, and abelian varieties (Amherst, MA, 1990)*, volume 136 of *Contemp. Math.*, pages 55–125. Amer. Math. Soc., Providence, RI, 1992.
[13] W. L. Edge. 28 real bitangents. *Proc. Roy. Soc. Edinburgh Sect. A*, 124(4):729–736, 1994.
[14] E. Victor Flynn. Electronic resources for curves of genus 2. available from `ftp://ftp.liv.ac.uk/pub/genus2/`, 1996.
[15] E.V. Flynn. The jacobian and formal group of a curve of genus 2 over an arbitrary ground field. *Math. Proc. Camb. Phil. Soc.*, 107:425–441, 1990.
[16] E.V. Flynn. A flexible method for applying chabauty's theorem. *Compositio Mathematica*, 105:79–94, 1997.
[17] William Fulton. *Algebraic curves. An introduction to algebraic geometry.* W. A. Benjamin, Inc., New York-Amsterdam, 1969. Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series.
[18] Robin Hartshorne. *Algebraic Geometry*. GTM 52. Springer-Verlag, 1977.
[19] David Mumford. Prym varieties. I. In *Contributions to analysis (a collection of papers dedicated to Lipman Bers)*, pages 325–350. Academic Press, New York, 1974.
[20] Sevin Recillas. Jacobians of curves with g_4^1's are the Prym's of trigonal curves. *Bol. Soc. Mat. Mexicana (2)*, 19(1):9–13, 1974.
[21] Edward F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, 310(3):447–471, 1998.
[22] Victor Scharaschkin. *Local-Global Problems and the Brauer-Manin Obstruction*. PhD thesis, University of Michigan, 1999.
[23] Alexei Skorobogatov. *Torsors and rational points*, volume 144 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2001.
[24] Alessandro Verra. The fibre of the Prym map in genus three. *Math. Ann.*, 276(3):433–448, 1987.
[25] Joseph L. Wetherell. *Bounding the number of rational points on certain curves of high rank*. PhD thesis, U.C. Berkeley, 1997.

Department of Mathematics, Simon Fraser University, Burnaby BC, Canada V5A 1S6
E-mail address: `bruin@member.ams.org`